Amendments to the Claims:

1. (currently amended) A method of securely downloading and installing patch data in a plurality of computing devices, each computing device having a processor, program memory and patch memory, said method comprising the steps of:

transmitting said patch data to said computing devices over a nonsecure channel in an encrypted manner utilizing a first key;

receiving first encrypted patch data at a computing device and decrypting said first encrypted patch data utilizing said first key ~~so as~~ to generate clear patch data;

verifying the integrity of the contents of said clear patch data; and if said verification passes,

encrypting said clear patch data using a second key and storing the resultant second encrypted patch data in a data memory;

retrieving said second encrypted patch data from said data memory and decrypting said second encrypted patch data using said second key ~~so as~~ to generate clear patch data; and

loading said clear patch data into said patch memory ~~and executing the contents thereof~~.

2. (original) The method according to claim 1, wherein said patch data is received from a satellite adapted to forward said patch data transmitted from a central data center.

3. (original) The method according to claim 1, wherein said patch data is received from a terrestrial repeater station adapted to forward said patch data transmitted from a central data center.

4. (original) The method according to claim 1, wherein said nonsecure channel comprises a satellite downlink.

5. (original) The method according to claim 1, wherein said nonsecure channel comprises a terrestrial wireless link.

6. (original) The method according to claim 1, wherein said computing device comprises the data processor portion of a radio receiver adapted to receive a signal transmitted from a satellite downlink.

7. (original) The method according to claim 1, wherein said computing device comprises the data processor portion of a radio receiver adapted to receive a signal transmitted from a terrestrial repeater station.

8. (original) The method according to claim 1, wherein said first key is known to all computing devices in said system.

9. (original) The method according to claim 1, wherein said first key is known to a portion of computing devices in said system.

10. (currently amended) The method according to claim 1, wherein each individual computing device comprises a unique said second key not ~~normally~~ known to other computing devices.

11. (original) The method according to claim 1, wherein said second encrypted patch data is stored in random access memory (RAM) integral to said device.

12. (original) The method according to claim 1, wherein said second encrypted patch data is stored in random access memory (RAM) located in a host device in communication with said computing device.

13. (original) The method according to claim 1, wherein said second encrypted patch data is stored in nonvolatile memory (NVM) integral to said device.

14. (original) The method according to claim 1, wherein said second encrypted patch data is stored in nonvolatile memory (NVM) located in a host device in communication with said computing device.

15. (original) The method according to claim 1, further comprising the step of deleting said patch information from said device in the event said verification fails.

16. (original) The method according to claim 1, further comprising the step of deleting said patch information from said device and subsequently rebooting said device in the event said verification fails.

17. (original) The method according to claim 1, wherein said first key is hardwired within said computing device.

18. (original) The method according to claim 1, wherein said second key is hardwired within said computing device.

19. (original) The method according to claim 1, wherein said second key is stored in nonvolatile memory external to said computing device.

20. (original) The method according to claim 1, wherein said second key is derived from a unique ID burnt into said computing device.

21. (currently amended) ~~Apparatus~~ An apparatus for securely downloading and installing patch data in a plurality of computing devices, said patch data transmitted over [[an]] a nonsecure channel in an encrypted manner using a first key, comprising:

patch memory adapted to store said patch data;

data memory;

a processor;

software means operative on said processor for:

receiving a first encrypted patch data transmitted to said computing devices and decrypting said first encrypted patch data utilizing said first key ~~so as~~ to generate clear patch data;

verifying the integrity of the contents of said clear patch data; and if said verification passes,

encrypting said clear patch data using a second key and storing the resultant second encrypted patch data in said data memory;

retrieving said second encrypted patch data from said data memory and decrypting said second encrypted patch data using said second key ~~so as~~ to generate clear patch data; and

loading said clear patch data into said patch memory ~~and executing the contents thereof~~.

22. (original) The apparatus according to claim 21, wherein said patch data is received from a satellite adapted to forward said patch data transmitted from a central data center.

23. (original) The apparatus according to claim 21, wherein said patch data is received from a terrestrial repeater station adapted to forward said patch data transmitted from a central data center.

24. (original) The apparatus according to claim 21, wherein said nonsecure channel comprises a satellite downlink.

25. (original) The apparatus according to claim 21, wherein said nonsecure channel comprises a terrestrial wireless link.

26. (original) The apparatus according to claim 21, wherein said computing device comprises the data processor portion of a radio receiver adapted to receive a signal transmitted from a satellite downlink.

27. (original) The apparatus according to claim 21, wherein said computing device comprises the data processor portion of a radio receiver adapted to receive a signal transmitted from a terrestrial repeater station.

28. (original) The apparatus according to claim 21, wherein said first key is known to all computing devices in said system.

29. (original) The apparatus according to claim 21, wherein said first key is known to a portion of computing devices in said system.

30. (currently amended) The apparatus according to claim 21, wherein each individual computing device comprises a unique second key not ~~normally~~ known [[by]] to other computing devices.

31. (original) The apparatus according to claim 21, wherein said data memory comprises random access memory (RAM) integral to said computing device.

32. (original) The apparatus according to claim 21, wherein said data memory comprises random access memory (RAM) located in a host device in communication with said computing device.

33. (original) The apparatus according to claim 21, wherein data memory comprises nonvolatile memory (NVM) integral to said device.

34. (original) The apparatus according to claim 21, wherein said data memory comprises nonvolatile memory (NVM) located in a host device in communication with said computing device.

35. (original) The apparatus according to claim 21, wherein said software means is operative to delete said patch information from said device in the event said verification fails.

36. (original) The apparatus according to claim 21, wherein said software means is operative to delete said patch information from said device and subsequently reboot said computing device in the event said verification fails.

37. (original) The apparatus according to claim 21, wherein said first key is hardwired within said computing device.

38. (original) The apparatus according to claim 21, wherein said second key is hardwired within said computing device.

39. (original) The apparatus according to claim 21, wherein said second key is stored in nonvolatile memory external to said computing device.

40. (original) The apparatus according to claim 21, wherein said second key is derived from a unique ID unique among all computing devices and permanently burnt into said computing device.

41. (currently amended) A system for downloading and installing patch data on a plurality of communication platforms, comprising:

transmission means for transmitting said patch data over a nonsecure link to said plurality of communication platforms wherein said patch data is transmitted encrypted utilizing a first key;

receiving means in each communications platform adapted to receive said patch data over said link;

a data processor adapted to receive said encrypted patch data from said receiving means;

a host device adapted to communicate with said data processor; and

said data processor comprising:

patch memory adapted to store said patch data;

data memory;

processing means;

software means operative on said data processor for:

receiving a first encrypted patch data transmitted at a computing device and decrypting said first encrypted patch data utilizing said first key ~~so as~~ to generate clear patch data;

verifying the integrity of the contents of said clear patch data; and if said verification passes,

encrypting said clear patch data using a second key and storing the resultant second encrypted patch data in said data memory;

retrieving said second encrypted patch data from said data memory and decrypting said second encrypted patch data using said second key ~~so as~~ to generate clear patch data; and

loading said clear patch data into said patch memory ~~and executing the contents thereof~~.

42. (original) The system according to claim 41, wherein said transmission means comprises means for transmitting said patch data from a central data center via a satellite to said plurality of communication platforms.

43. (original) The system according to claim 41, wherein said transmission means comprises means for transmitting said patch data from a central data center via a terrestrial repeater station to said plurality of communication platforms.

44. (original) The system according to claim 41, wherein said nonsecure link comprises a satellite downlink.

45. (original) The system according to claim 41, wherein said nonsecure link comprises a terrestrial wireless link.

46. (original) The system according to claim 41, wherein said communications platform comprises a portable or fixed radio operative to receive, demodulate and decode a signal broadcast via satellite.

47. (original) The system according to claim 41, wherein said communications platform comprises a portable or fixed radio operative to receive, demodulate and decode a signal broadcast via a terrestrial repeater station.

48. (original) The system according to claim 41, wherein said first key is known to all communications platforms in said system.

49. (original) The system according to claim 41, wherein said first key is known to a portion of communications platforms in said system.

50. (currently amended) The system according to claim 41, wherein each individual communications platform comprises a unique second key not ~~normally~~ known [[by]] to other communications platforms.

51. (original) The system according to claim 41, wherein said data memory comprises random access memory (RAM) integral to said data processor.

52. (original) The system according to claim 41, wherein said data memory comprises random access memory (RAM) coupled to said host device.

53. (original) The system according to claim 41, wherein data memory comprises nonvolatile memory (NVM) integral to said data processor.

54. (original) The system according to claim 41, wherein said data memory comprises nonvolatile memory (NVM) coupled to said host device.

55. (original) The system according to claim 41, wherein said software means is operative to delete said patch information from said communication platform in the event said verification fails.

56. (original) The system according to claim 41, wherein said software means is operative to delete said patch information from said communication platform and subsequently reboot said communication platform in the event said verification fails.

57. (original) The system according to claim 41, wherein said first key is hardwired within said data processor.

58. (original) The system according to claim 41, wherein said second key is hardwired within said data processor.

59. (original) The system according to claim 41, wherein said second key is stored in nonvolatile memory external to said data processor.

60. (original) The system according to claim 41, wherein said second key is derived from an ID unique among all communication platforms and permanently burnt into said data processor.

61. (new) A method of securely downloading a patch in a plurality of computing devices each having a processor, program memory and patch memory, said method comprising the steps of:

transmitting said patch encrypted utilizing a first key to said plurality of computing devices over a nonsecure channel, wherein said first key shared among said plurality of computing devices;

receiving a first encrypted patch at a computing device and decrypting said first encrypted patch utilizing said first key to generate a first clear patch;

verifying the integrity of said first clear patch; and if said verification is successful,

encrypting said first clear patch using a second key, wherein each computing device has a second key unique thereto; and

storing the second encrypted patch in a data memory.

62. (new) The method of claim 61, further comprising the steps of:

retrieving said second encrypted patch from said data memory;

decrypting said second encrypted patch using said second key to generate a second clear patch; and

loading said second clear patch into said patch memory.

63. (new) An apparatus for securely downloading a patch in a plurality of computing devices, said patch data transmitted over a nonsecure channel in an encrypted manner using a first key shared among said plurality of computing devices, comprising:

a processor;

patch memory coupled to said processor and adapted to store said patch;

data memory coupled to said processor;

software means operative on said processor to:

receive a first encrypted patch at a computing device and decrypt said first encrypted patch utilizing said first key to generate a first clear patch;

verify the integrity of said first clear patch; and if said verification is successful,

encrypt said first clear patch using a second key, wherein each computing device has a second key unique thereto; and

store the second encrypted patch in a data memory.

64. (new) The apparatus of claim 63, wherein said software means is further operative to:

retrieve said second encrypted patch from said data memory;

decrypt said second encrypted patch using said second key to generate a second clear patch; and

load said second clear patch into said patch memory.